**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Original) A cryptographic system in a computer system, comprising:

at least one server; and

at least one secret value including a master key, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key, the parts being encrypted by a password-derived or token-based key, each part being associated with a password wherein the at least one server can update the master key by requiring only some of the passwords to be revealed.

2. (Original) A cryptographic system as in claim 1, wherein the master key is used for protecting sensitive information processed by the at least one server.

3. (Original) A cryptographic system as in claim 1 further comprising a database, wherein the sensitive information is stored in the database.

4. (Original) A cryptographic system as in claim 1 in which the master key is split into the two or more parts according to the Bloom-Shamir methodology.

5. (Currently amended) A method used in a cryptographic system including a server, comprising:

providing at least one secret value including a master key;

splitting the master key into two or more parts wherein fewer than all the parts are required for reassembling the master key; and

encrypting the parts by a password-derived or token-based key, each part being associated with a password, wherein the master key can be reassembled by the server by requiring only some of the passwords to be revealed.

6. (Currently amended) A method as in claim 5, wherein the master key is used for protecting sensitive information processed by ~~a~~ the server in the cryptographic system.

7. (Original) A method as in claim 5 wherein the master key is split into the two or more parts according to the Bloom-Shamir methodology.

8. (New) A server, comprising:

a storage area for storing a at least one secret value including a master key, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key, the parts being encrypted by a password-derived or token-based key, each part being associated with a password; and

means for updating the master key by requiring only some of the passwords to be revealed.

9. (New) A server as defined in claim 8, further comprising an input coupled to the means for updating the master key, the input receiving some of the passwords.

10. (New) A server as defined in claim 9, wherein some of the passwords are received from a plurality of clients coupled to the server.